

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

Mikael Marczak, a/k/a Michael Marczak,
individually, also d/b/a Virtual PC Solutions, First
PC Solution, Direct PC Solution, Virtual IT
Supports, and Global Innovative Services, and

Wahid Ali, individually, and as a manager of
Virtual PC Solutions and Global Innovative
Services,

Defendants.

Case No. _____

**COMPLAINT FOR PERMANENT
INJUNCTION AND OTHER
EQUITABLE RELIEF**

Plaintiff, the Federal Trade Commission (“FTC”), for its Complaint alleges:

1. The FTC brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b) and 57b, and the Telemarketing and Consumer Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. §§ 6101-6108, as amended, to obtain temporary, preliminary, and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for the Defendants’ acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the FTC’s Telemarketing Sales Rule (“TSR”), 16 C.F.R. Part 310, as amended.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and

1345, and 15 U.S.C. §§ 45(a), 53(b), 57b, 6102(c), and 6105(b).

3. Venue is proper in this district under 28 U.S.C. § 1391(b), (c), and (d), and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101-6108, as amended. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 56(a)(2)(A)-(B), 57b, 6102(c), and 6105(b).

DEFENDANTS

6. Defendant Mikael Marczak, a/k/a Michael Marczak, operates the scheme described below using several different business names, including Virtual PC Solutions, First PC Solution, Direct PC Solution, Virtual IT Supports, and Global Innovative Services. He is also the registered owner of the fictitious names Virtual PC Solutions, First PC Solution, Direct PC Solution, and Virtual IT Supports, and holds himself out as the Sales Director of Global Innovative Services. At all times material to this Complaint, acting alone or in concert with others, he has advertised, marketed, distributed, or sold computer security or technical support

services to consumers throughout the United States. The Defendant Mikael Marczak resides in California, and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

7. Defendant Wahid Ali is the Operations Manager of Virtual PC Solutions and holds himself out as the CEO of Global Innovative Services. At all times material to this Complaint, acting alone or in concert with others, he has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States. Defendant Wahid Ali resides in Kolkata, India, and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

COMMERCE

8. At all times material to this Complaint, the Defendants have maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS’ BUSINESS ACTIVITIES

Overview

9. The Defendants operate a massive telemarketing scheme that tricks consumers into spending from \$79 - \$429 to fix non-existent problems with their computers. By exploiting consumers’ legitimate concerns about Internet threats like spyware and viruses, the Defendants scare consumers into believing that their computers are in imminent danger of crashing in order to sell consumers otherwise free software protection products and unnecessary computer security or technical support services.

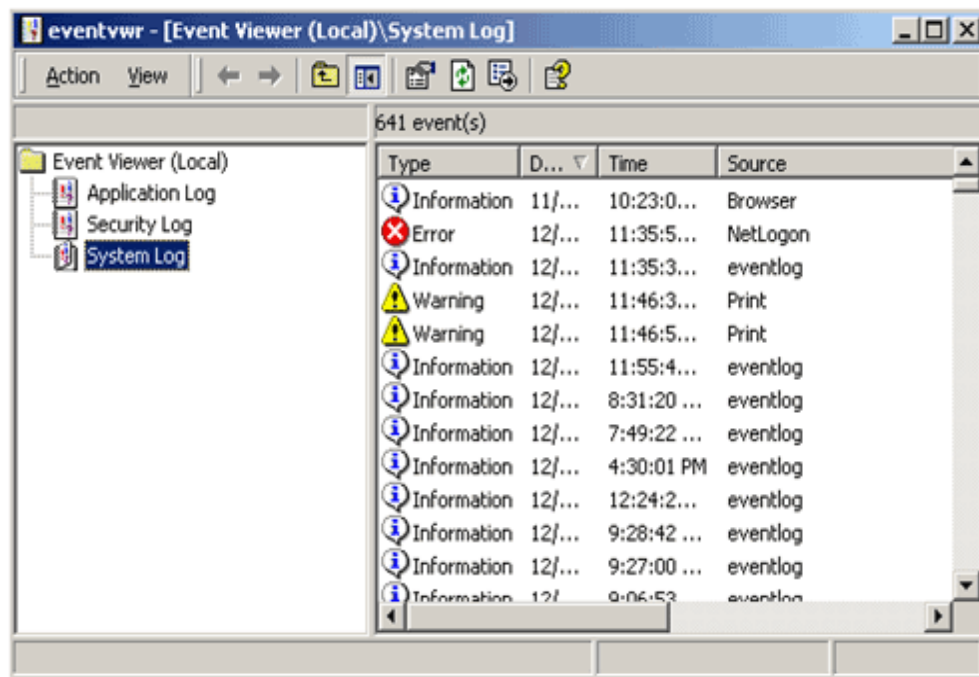
Defendants Lure Consumers to Purchase Their Services

10. Since at least 2011, the Defendants have been cold calling consumers in the United States

and other English speaking countries and falsely claiming that they are from or affiliated with well-known computer manufacturers or computer security companies such as Microsoft or Dell.

11. After the Defendants have tricked the consumers into thinking they are dealing with their computer manufacturer or a computer security company, the Defendants scare the consumers into believing that they have viruses or other malware on their computers.

12. To mislead the consumers into believing that their computers are infected with viruses or other malware, the Defendants direct the consumers to a program on their computer called the Event Viewer. The Event Viewer is a log of the various activities that occur during a computer's operation. Many of the entries in the Event Viewer simply reflect that a computer operation was completed successfully. Other entries, marked with a red x or a yellow triangle, are error or warning messages that indicate that a particular computer operation was not successful. If, for example, a program failed to run correctly because the user was not connected to the Internet, the Event Viewer may record an error or warning message. Despite their potentially alarming appearance, these messages are innocuous. They are generated during the normal operation of a computer. A screenshot of a sample Event Viewer appears below:



13. After directing the consumer to the Event Viewer, the Defendants often will ask the consumers if they see any entries with errors or warnings marked with red x's and yellow triangles. When the consumers respond that they do, the Defendants will state that these entries confirm that there are viruses or other malware present on the consumers' computers and that the computers are in danger of crashing.

14. This claim is baseless. It is impossible to know whether or not a computer is infected with viruses or malware based solely on the fact that the computer's Event Viewer contains warning or error messages. Computers that are completely free of viruses or other malware will still create warning and error messages in their Event Viewers during normal operation. The Defendants mislead consumers who do not understand these messages' technical significance into believing that their computers are severely compromised.

15. Having convinced the consumers that their computers are in imminent danger, the

Defendants then direct the consumers to a website and instruct them to enter a code or download a software application to allow the Defendants remote access to the consumers' computers.

Once the Defendants have remote access, they are able to completely control the consumers' computers and can, for example, move the cursor, enter commands, run applications, and access stored information.

16. After gaining remote access, the Defendants continue their deception by focusing the consumer's attention on a list of innocuous files, emphasizing the risk these files supposedly pose, and stressing the urgent need for the consumer to buy the Defendants' products and services to prevent the computer from crashing.

17. The Defendants then attempt to sell the consumer illusory long-term "security" or "technical support" services and perform unnecessary "repairs," including installing otherwise free programs, such as trial versions of antivirus programs, and deleting the innocuous files they falsely claimed were viruses. The Defendants charge consumers for these services in an amount ranging from approximately \$79 to \$429.

18. The Defendants next direct the consumer to one of several websites they operate in order to pay for the computer security or technical support service. The Defendants' websites are highly interactive. They purport to allow consumers to chat directly with representatives, leave their contact information to request a call-back, and also browse and pay for various services online.

19. If consumers do not agree to pay for the service, the Defendants typically apply pressure to the consumers. The Defendants will warn consumers about the harm that will come to their computers if they do not allow the Defendants remote access to fix the computers.

20. Afterwards, the Defendants assert they have fixed the non-existent problems. In reality,

Defendants merely charged consumers for repair products and services they did not need.

21. In numerous instances, the Defendants call consumers who are registered on the National Do Not Call Registry.

22. In numerous instances, the Defendants call consumers who are within a given area code when the Defendants have not paid the required annual fee for access to telephone numbers within that area code that are included in the National Do Not Call Registry.

23. To hide their true identities, the Defendants utilize multiple websites and fictitious names.

The Role of Mikael Marczak

24. Defendant Mikael Marczak is the registered owner of the fictitious names Virtual PC Solutions, First PC Solution, Direct PC Solution, and Virtual IT Supports, and holds himself out as the Sales Director of Global Innovative Services. Marczak established merchant accounts at First Data and IPayment for First PC Solution, and set up a PayPal account for Virtual PC Solutions. In addition, he registered and paid for First PC Solution and Direct PC Solution domains through Go Daddy.

The Role of Wahid Ali

25. Defendant Wahid Ali is the Operations Manager of Virtual PC Solutions and holds himself out as the CEO of Global Innovative Services. Ali set up a PayPal account used by Virtual PC Solutions to process consumers' credit cards, and, using the user name VirtualITSupports, he subscribed to the phone number on Virtual PC Solutions' website. Moreover, he established an Amazon merchant account for Virtual PC Solutions.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

26. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or

practices in or affecting commerce.”

27. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

Count I

Deceptive Representations

28. In numerous instances, in the course of marketing, offering for sale, and selling computer security or technical support services, the Defendants represent or have represented, expressly or by implication, through a variety of means, including telephone calls and Internet communications, that they have detected security or performance issues on consumers’ computers, including viruses, spyware, or system errors.

29. In truth and in fact, in numerous instances in which the Defendants have made the representations set forth in Paragraph 28, the Defendants have not detected security or performance issues on consumers’ computers.

30. Therefore, the Defendants’ representations as set forth in Paragraph 28 are false, misleading, or were not substantiated at the time they were made, and thus, they constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II

Deceptive Representations

31. In numerous instances, in the course of marketing, offering for sale, and selling computer security or technical support services, the Defendants represent or have represented, expressly or by implication, through a variety of means, including telephone calls and Internet communications, that they are from, affiliated with, or calling on behalf of a well-known computer company such as Microsoft or Dell.

32. In truth and in fact, Defendants are not from, affiliated with, or calling on behalf of the well-known computer company.

33. Therefore, the Defendants' representations as set forth in Paragraph 31 are false or misleading, and thus, they constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

34. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101-6108, in 1994. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively amended it in 2003, and amended certain provisions thereafter.

35. The Defendants are sellers or telemarketers engaged in "telemarketing" as defined by the TSR, 16 C.F.R. § 310.2(aa), (cc), and (dd).

36. The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 C.F.R. § 310.3(a)(4).

37. Among other things, amendments made to the TSR in 2003 established a do not call registry (the "National Do Not Call Registry"), maintained by the FTC, of consumers who do not wish to receive certain types of telemarketing calls. Consumers can register their telephone numbers on the National Do Not Call Registry without charge either through a toll-free telephone call or over the Internet at *donotcall.gov*.

38. Consumers who receive telemarketing calls to their registered numbers can complain of National Do Not Call Registry violations the same way they registered, through a toll-free telephone call or over the Internet at *donotcall.gov*, or by otherwise contacting law enforcement

authorities.

39. The FTC allows sellers, telemarketers, and other permitted organizations to access the National Do Not Call Registry over the Internet at *telemarketing.donotcall.gov*, to pay the fee(s) if required, and to download the numbers not to call.

40. Under the TSR, “outbound telephone call” means a telephone call initiated by a telemarketer to induce the purchase of goods or services or to solicit a charitable contribution. 16 C.F.R. § 310.2(v).

41. The TSR prohibits sellers and telemarketers from initiating an outbound telephone call to numbers on the National Do Not Call Registry. 16 C.F.R. § 310.4(b)(1)(iii)(B).

42. The TSR prohibits sellers and telemarketers from calling any telephone number within a given area code unless the seller on whose behalf the call is made has paid the annual fee for access to the telephone numbers within that area code that are included in the National Do Not Call Registry. 16 C.F.R. § 310.8.

43. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count III

Deceptive Telemarketing Calls in Violation of the TSR

44. In numerous instances, in the course of telemarketing their goods and services, the Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that they have detected security or performance issues on consumers’ computers, including viruses,

spyware, or system errors.

45. The Defendants' acts or practices, as described in Paragraph 44 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

Count IV

Deceptive Telemarketing Calls in Violation of the TSR

46. In numerous instances, in the course of telemarketing their goods and services, the Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that they are from, affiliated with, or calling on behalf of a well-known computer company such as Microsoft or Dell.

47. The Defendants' acts or practices, as described in Paragraph 46 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

Count V

Violating the National Do Not Call Registry

48. In numerous instances, in connection with telemarketing, the Defendants initiated or caused others to initiate an outbound telephone call to a person's telephone number on the National Do Not Call Registry in violation of the TSR, 16 C.F.R. § 310.4(b)(1)(iii)(B).

Count VI

Failing to Pay the National Registry Fees

49. In numerous instances, in connection with telemarketing, the Defendants have initiated, or caused others to initiate, an outbound telephone call to a telephone number within a given area code when the Defendants had not, either directly or through another person, paid the required annual fee for access to the telephone numbers within that area code that are included in the

National Do Not Call Registry, in violation of the TSR, 16 C.F.R. § 310.8.

CONSUMER INJURY

50. Consumers have suffered and will continue to suffer substantial injury as a result of the Defendants' violations of the FTC Act and the TSR. In addition, the Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, the Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

51. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

52. Section 19 of the FTC Act, 15 U.S.C. § 57b, and Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the TSR, including the rescission or reformation of contracts, and the refund of money.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, the TSR, and the Court's own equitable powers, requests that the Court:

A. Award Plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to

preserve the possibility of effective final relief, including but not limited to temporary and preliminary injunctions, and an order providing for the turnover of business records, immediate access to documents, an asset freeze, and the disruption of domain and telephone services;

B. Enter a permanent injunction to prevent future violations of the FTC Act and the TSR by the Defendants;

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the FTC Act and the TSR, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

D. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

WILLARD K. TOM
General Counsel

Dated: September 24, 2012

/s Kelly Horne
Kelly Horne, CA Bar #242675
Colleen B. Robbins, SDNY Bar #CB5086
Christine M. Todaro, OH Bar #0084976
Benjamin R. Davidson, DC Bar #975509
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3031; khorne@ftc.gov
(202) 326-2548; crobbins@ftc.gov
(202) 326-3711; ctodaro@ftc.gov
(202) 326-3055; bdavidson@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION